



# **IT GOVERNANCE:**

**The Way Ahead**

**BSI Conference**

**20 May 2009**

**Alan Calder**

**IT Governance Ltd**

**[www.itgovernance.co.uk](http://www.itgovernance.co.uk)**

# OVERVIEW



- Emerging Trends
- Data Protection and IT governance
- Aligning Board, Management and Auditors
- Integrating IT Standards – the IT Management System of Tomorrow
- Preparing for the upturn

# Current reality



- **ITGI Survey 2009**
  - *Half of the respondents indicate that **IT is very important to the enterprise, and three-quarters align IT and business strategies.** Yet IT matters are discussed **predominantly on an ad hoc basis at the board level.***
  - *Those in IT management believe they provide the business side of the enterprise with frequent information about new technology opportunities, but the business side does not seem to receive this information.*
- **Enterprise Management Associates 2008**
  - The guidance most frequently adopted by all respondents is not a risk or compliance control framework. It is the process-centric IT Infrastructure Library. Some version of ITIL has been adopted by 55% of all respondents—19% ahead of the next most frequently referenced guidance
  - That next-most-frequent guidance is not specific to IT management *per se*. *It is in quality management.* 36% of all respondents have adopted quality management standards such as Six Sigma or the ISO 9000 series.
  - These numbers compare to rates of adoption of 30% for the ISO 27000-series and related BS 7799 risk management standards, 29% for COBIT, and 11% for COSO.

**New trends are a bit like the old trends**

# What does that mean?

- IT Governance professionals still have a major strategic sales job to do.....
  - Business value of IT governance frameworks
  - Necessity for directors to be involved in IT governance
- Responsibility for IT governance still to be clarified
  - Most respondents acknowledge that **executive management is accountable for IT governance (ITGI Survey 2009)**
  - "The system by which business corporations are directed and controlled" (OECD 1999)
  - *Corporate governance of IT involves evaluating and directing the use of IT to support the organisation (ISO/IEC 38500)*
  - Which means that directors have a key role to play in IT governance
  - But how do we get boards involved?

# Emerging issues

- Still emergent
  - Dematerialised perimeter
  - SoA (Service Orientated Architecture)
  - IT and Enterprise Architectures
- Hot issues
  - Virtualisation
  - Cloud Computing
    - SaaS
- Social Networking, Web 2.0
- Green IT [www.itgovernance.co.uk/green-it.aspx](http://www.itgovernance.co.uk/green-it.aspx)

# Data Protection & IT Governance



- Boards are expected to ensure that laws are obeyed and significant risks mitigated
  - Data Protection Act 1998 to be supported by an ICO with powers to levy 'substantial fines' on organisations that he considers guilty of 'reckless disregard' of DPA
  - BS10012 – specification for a 'PIMS'
  - PCI DSS exposes e-commerce organisations to potentially substantial penalties for failing to protect cardholder data
- Risks involve information and, therefore, information technology
  - Governance of IT helps boards tackle these risks

<http://www.itgovernance.co.uk/data-protection.aspx>

# Proliferation of Standards and Frameworks



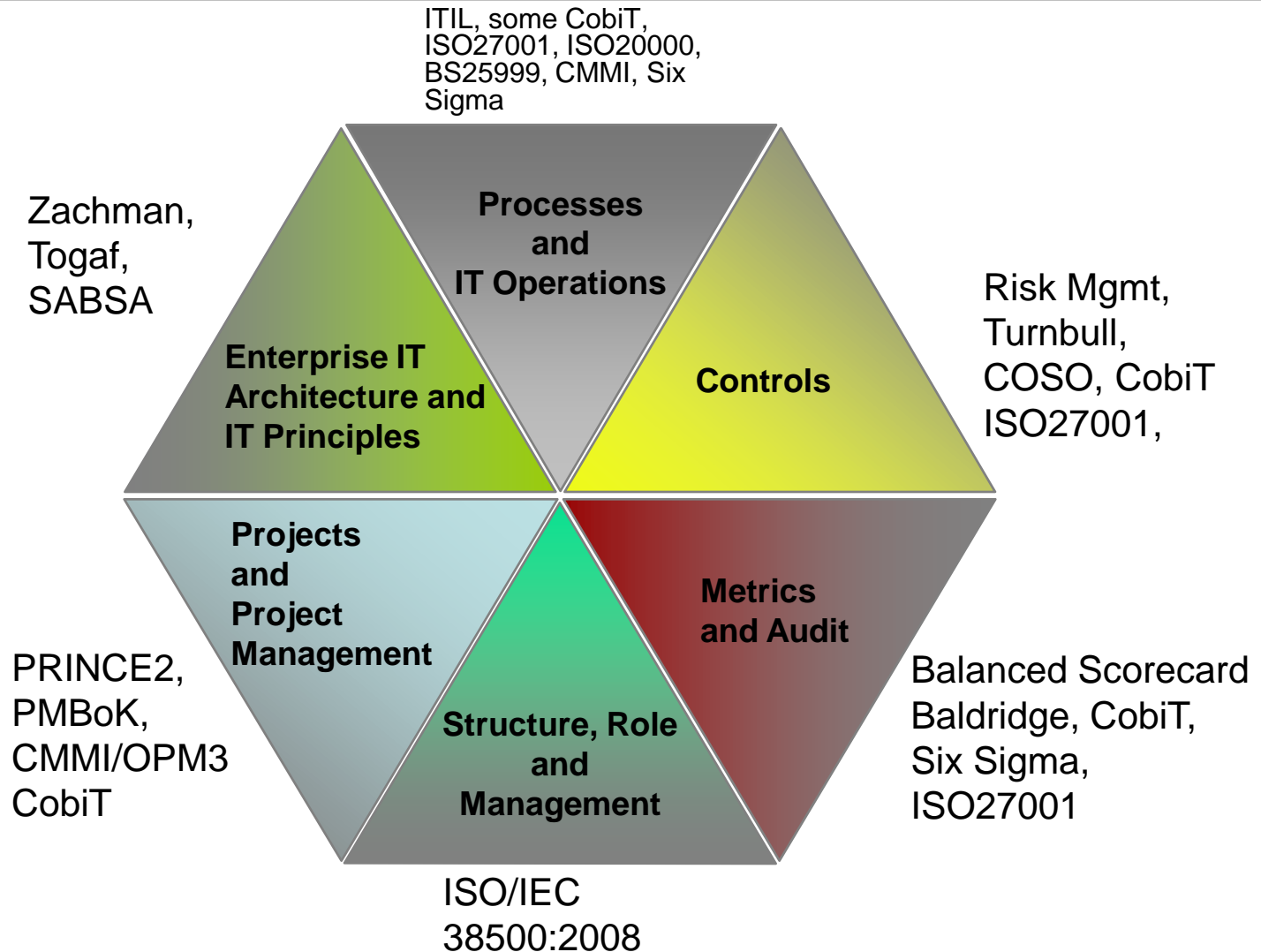
- Management System Standards
  - ISO/IEC 38500 [www.itgovernance.co.uk/iso38500.aspx](http://www.itgovernance.co.uk/iso38500.aspx)
  - ISO/IEC 27000 [www.itgovernance.co.uk/iso27001.aspx](http://www.itgovernance.co.uk/iso27001.aspx)
  - ISO/IEC 20000 [www.itgovernance.co.uk/iso20000.aspx](http://www.itgovernance.co.uk/iso20000.aspx)
  - BS25999/BS25777 - ISO/IEC 24762
  - BS 31100
- Proprietary Frameworks
  - CoBIT and ValIT
  - ITIL
  - PRINCE2, P3O, PMBoK, MSP, M\_o\_R
- Enterprise Architecture Frameworks
  - TOGAF [www.itgovernance.co.uk/togaf.aspx](http://www.itgovernance.co.uk/togaf.aspx)
- Quality Management Frameworks
  - Six Sigma, CMMI, ISO9001, ISO14001

# CoBIT linkages

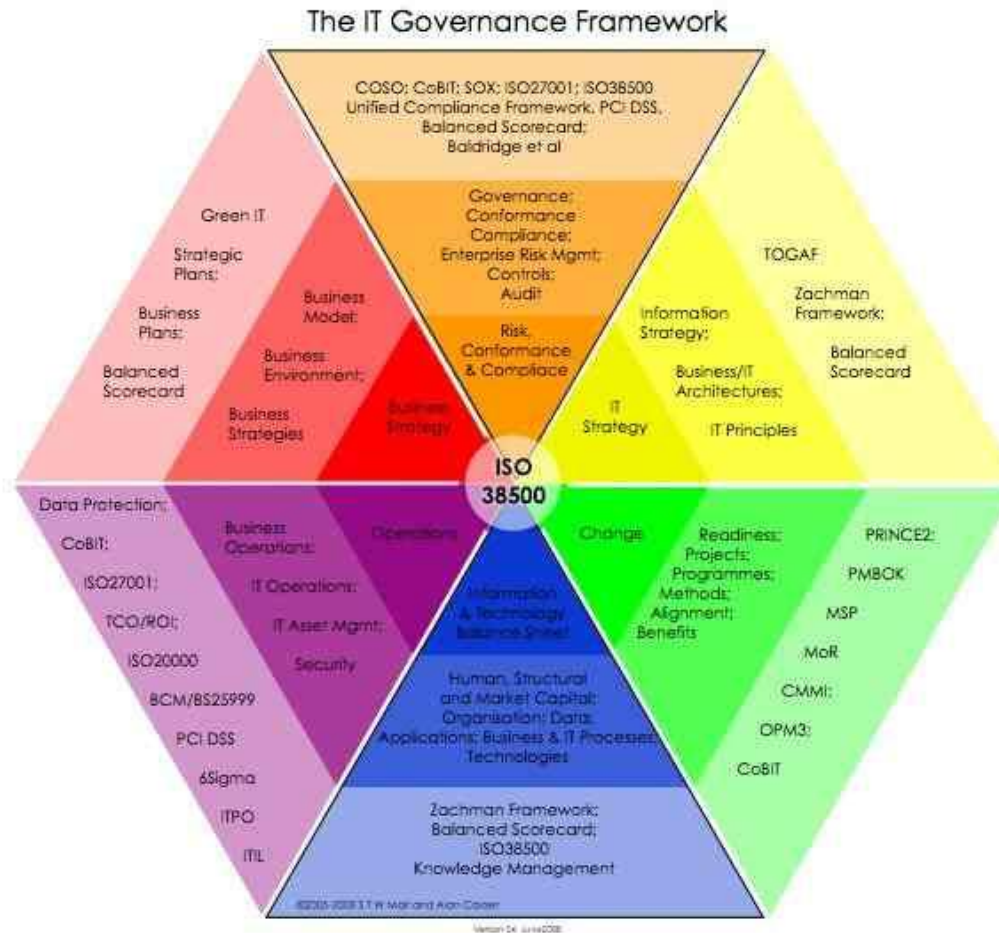


- ITGI™ Enables ISO/IEC 38500:2008 Adoption
  - *'summarizes how COBIT, Val IT and related guidance support adoption of the standard's principles and implementation approach'*
- Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit
- COBIT Mapping Overview of International IT Guidance 2nd Edition (now out of date)
- <http://www.itgovernance.co.uk/cobit.aspx>

# The IT Governance Toolbox



# The Calder-Moir Framework

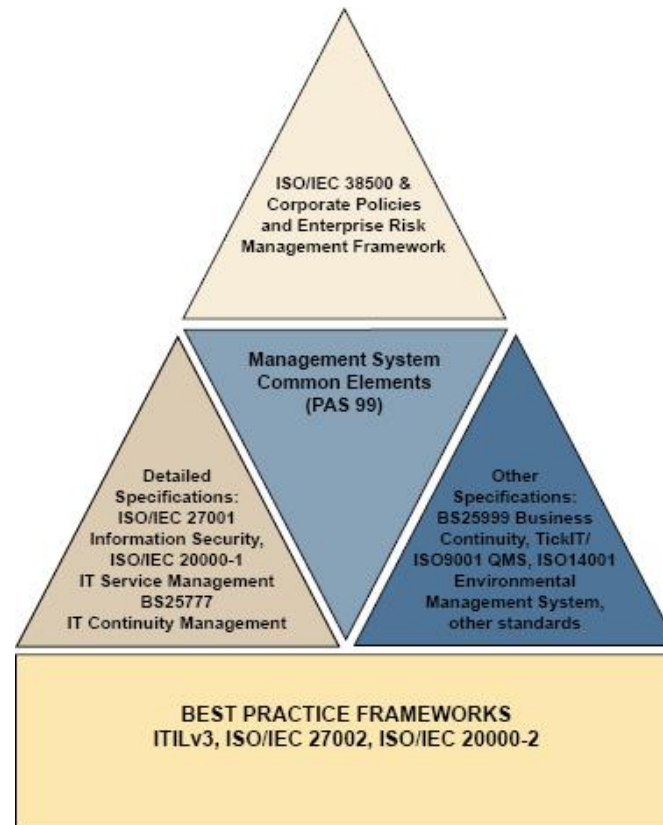


[www.itgovernance.co.uk/calder\\_moir.aspx](http://www.itgovernance.co.uk/calder_moir.aspx)

IT Governance Framework Toolkit: [www.itgovernance.co.uk/products/519](http://www.itgovernance.co.uk/products/519)

# Integrating IT Standards

- *The IT Management System of Tomorrow*
  - *New Book by Alan Calder, published by BSI in Autumn 2009*

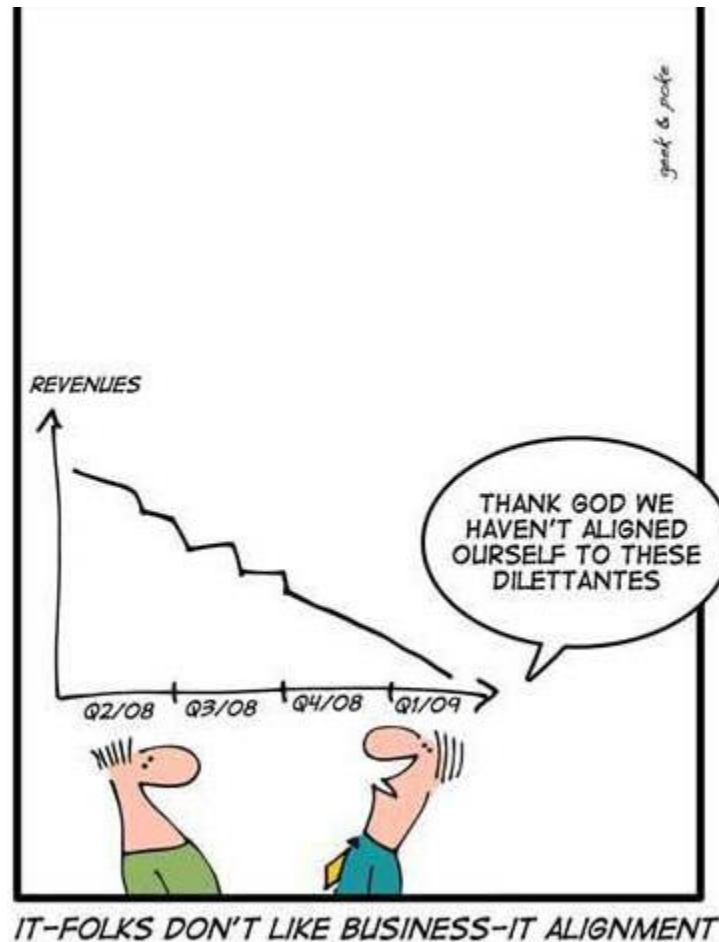


# The Bigger Issues



- Governance is not management
  - Governance is about oversight – and frameworks simplify oversight
  - Key role for non-executives
  - Public sector usage confuses
- Proliferation of IT areas for ‘governance’
  - But no HR governance, sales governance.....
- Communication
  - Which should be a two-way process

# That was the downturn....



# Getting Board Buy-in

- Start conversations about governance vs management
- Personalise generic risks to your own organisation
  - Better governance of Project X would produce Y result
  - Identify specific business benefits, with an ROI
- Find an interested member of the executive team or non-executive board member
- Be persistent

# Prepare for the upturn



- Four good reasons to embrace IT governance (CIO.com)
    1. Avoid project failure because risks are "properly measured and managed."
    2. Avoid those projects and initiatives that do not add value to the business strategy because those that are closely aligned with business strategy are promoted and those that are stopped early
    3. Measure the cost and quality of projects as they are in process.
    4. Improves transparency in and accountability for IT
- IT Governance, in other words, brings a competitive edge to organisations – those with good IT governance frameworks are likely to emerge from the recession faster and fitter than their competitors.

# Resources



- Standards, books and tools (The One-Stop-Shop for: ISO/IEC38500, ITIL, ISO/IEC 20000, ISO/IEC 27001, CobiT, PRINCE2, PMBoK, IT Service Management, Knowledge Management, Intellectual Capital, Business Continuity etc):

[www.itgovernance.co.uk](http://www.itgovernance.co.uk)